報道関係者各位

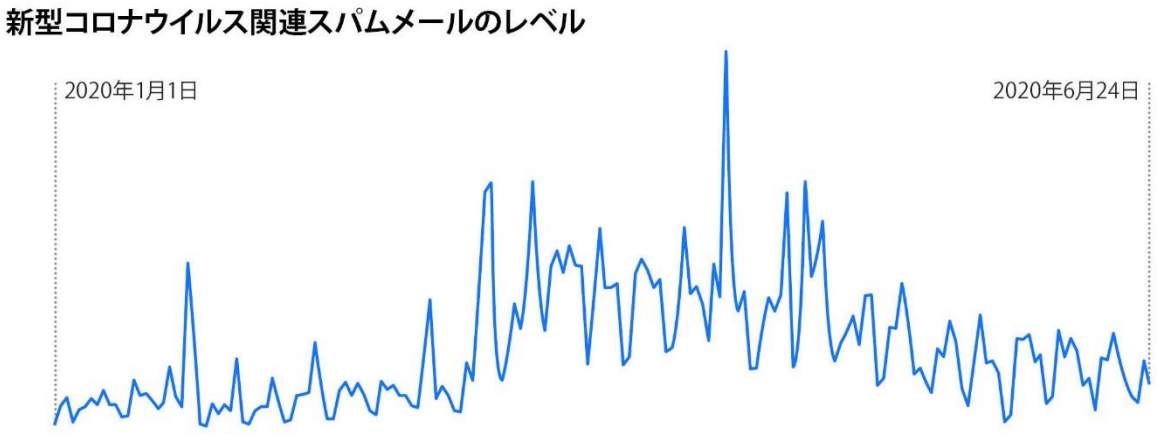
新型コロナウイルス関連のフィッシング攻撃を多数観測、エフセキュアが 2020 年上半期の攻撃トラフィックレポートを発表

～ 人々が持つ新型コロナウイルスへの恐れや社会的混乱を悪用～

2020 年 9 月 15 日
エフセキュア株式会社

先進的サイバー・セキュリティ・テクノロジーのプロバイダーである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Samu Konttinen、日本法人: 東京都港区、以下、エフセキュア) は本日、2020 年上半期 (1 月～6 月) における攻撃トラフィックに関する調査レポートを発表しました。同期間において発生した新型コロナウイルスの世界的なパンデミックは、多くの人々の生活や企業の業務を混乱に導いただけでなく、スパムやフィッシングメールを介したサイバー攻撃のアシストをするかたちとなってしまいました。

エフセキュアの『セキュリティ脅威のランドスケープ　2020 年上半期』レポートによると、同期間のオンライン脅威のトラフィックを調査した結果、サイバー犯罪者は新型コロナウイルスのパンデミックに乗じて迅速に行動を開始しました。3 月から 春にかけて、新型コロナウイルスに関連する様々なトピックを利用した悪質な E メールが大幅に増加しており、ユーザーをおびき寄せて様々な E メール攻撃や詐欺の被害に遭わせるように仕向けています。



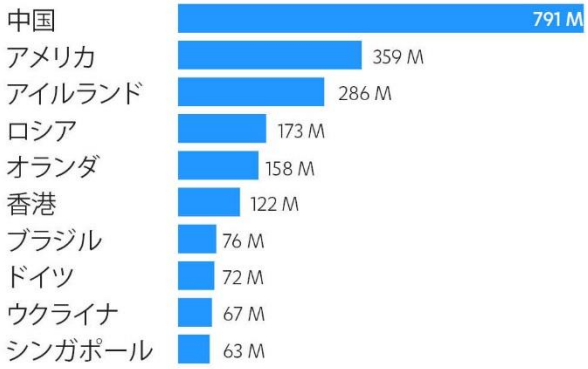
これらのメールを介した新型コロナウイルス関連の攻撃キャンペーンは、ユーザーを騙して偽の Web サイトからマスクを注文させようとするものや、悪意のある添付ファイルを開いてマルウェアに感染させようとするものまで、多岐に渡っていました。これらのメールに含まれる添付ファイルの 4 分の 3 以上には、感染したシステムからパスワードやその他の資格情報などの機密情報を盗み出すインフォスティーラー (情報搾取型マルウェア) が含まれていました。

エフセキュアの戦術防衛ユニット (Tactical Defense Unit) のマネージャーである Calvin Gan (カルビン・ガン) は、今回の調査について以下のように語っています。
「サイバー犯罪者には行動上の制約があまりないため、世の中に大きなインパクトを与える出来事に迅速に対応し、関連する要素を攻撃キャンペーンに組み込むことができます。新型コロナウイルスの発生当初、混乱が生じたり人々の間で不安が募るなか、攻撃者は予想通り、人々の不安を餌食にしようとしていました。企業においても、多忙な日々を送る社員にとって、悪意のある E メールの発見は通常業務における最優先事項ではないため、攻撃者は頻繁に彼らを騙してネットワークに侵入しようと試みるのです。」

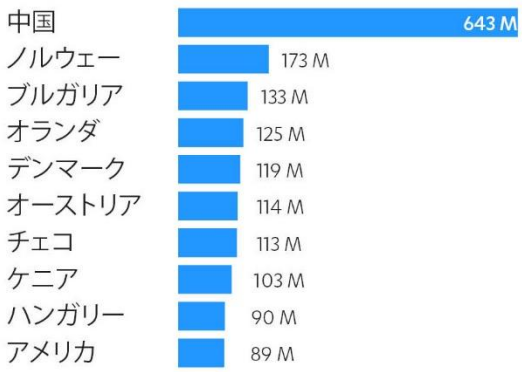
今回の調査からのその他ファクト

- 最も多くの攻撃を受けた国は中国、ノルウェー、ブルガリア、オランダ、デンマークの順。
- 攻撃の発信源として観測された国は中国、アメリカ、アイルランド、ロシア、オランダの順。
- 分野別のフィッシング詐欺は金融が最も多く、続いて SNS、オンラインサービス、決済サービス、E メールプロバイダーの順。社名／ブランド名別では Facebook、Chase Personal Banking、Microsoft Office 365、PayPal、Bank of America が上位を占める。
- E メールはマルウェアの拡散で最も広くも使用された手法で、感染の半数以上を占めていた。
- 攻撃者によって最も拡散されたマルウェアのタイプはインフォスティーラーであり、マルウェアファミリーとしては Lokibot が最多。
- TCP ポート別では Telnet が最も多く標的とされ、次点は SSH。

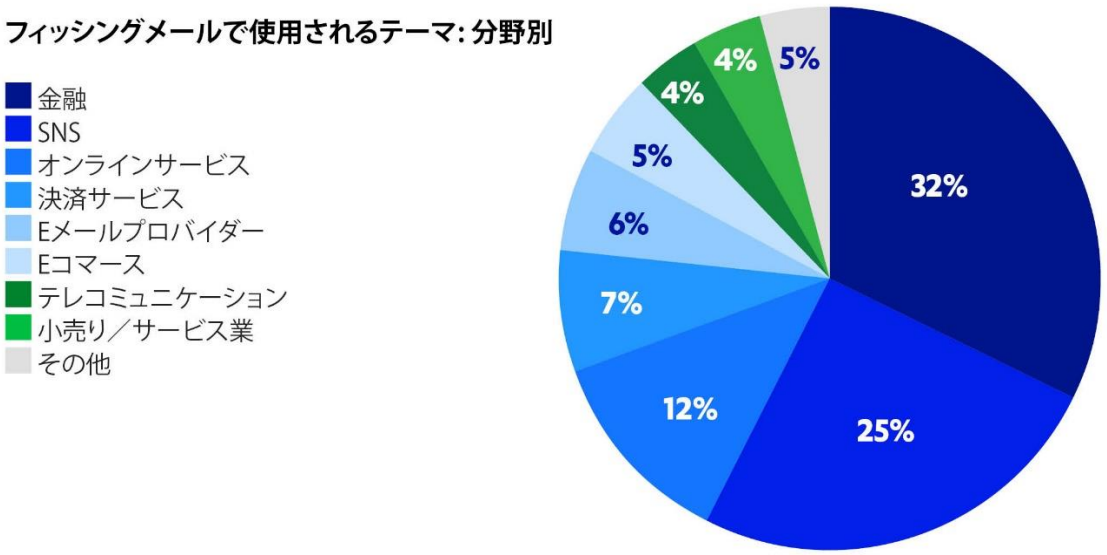
攻撃の発信源 (2020年上半期)



標的となった国 (2020年上半期)



フィッシングメールで使用されるテーマ: 分野別



また、クラウドベースのメールサービスを利用した攻撃が着実に増加しており、4 月には Microsoft Office 365 ユーザーを標的としたフィッシングメールが大幅に増加していることが観測されています。

エフセキュアで B2B 製品のマネジメントディレクターを務める Teemu Myllykangas (テーム・ミリカンガス) は、クラウドサービスへの攻撃について、次のように警告しています。
「クラウドサービスからの通知メッセージは通常のものであり、それを受信する従業員はそうした通知を信頼することに慣れています。攻撃者がその信頼を悪用して ターゲットを危険にさらすことは、企業がクラウドへの移行の際に対

処しなければならない最大の課題かもしれません。一般的に、受信トレイのセキュリティを確保することは既に課題となっているため、企業はセキュリティ技術と従業員教育を組み合わせた多層的なセキュリティアプローチを検討し、Eメールを介した脅威からのリスクを低減させる必要があります。」

レポートの全文（日本語版）は、以下よりダウンロードいただけます。
https://www.f-secure.com/jp-ja/press/media-library/reports
エフセキュア　プレスリリースページ:
https://www.f-secure.com/jp-ja/press

エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関するAIテクノロジー、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。
エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQヘルシンキに上場しています。詳細は https://www.f-secure.com/en/welcome（英語）および https://www.f-secure.com/ja_JP/（日本語）をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

※以下、メディア関係者限定の特記情報です。個人のSNS等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】

エフセキュア株式会社
広報部　　秦　和哉
TEL：03-4578-7745（直通）　　japan-pr@f-secure.com